# Multi-party Agile Quantum Key Distribution Network with a Broadband Fiber-based Entangled Source

**E. Y. Zhu,[*1], C. Corbari,[2] A.V. Gladyshev,[3] P. G. Kazansky,[2] H. K. Lo,[1,4] L. Qian[†1]**

[1]*Dept. of Electrical and Computer Engineering, University of Toronto, 10 King's College Rd., Toronto, ON M5S 3G4, Canada*
[2]*Optoelectronics Research Centre, University of Southampton, SO17 1BJ, United Kingdom*
[3]*Fiber Optics Research Center of the Russian Academy of Sciences, 119333, 38 Vavilov street, Moscow, Russia*
[4]*Dept. of Physics, University of Toronto, 60 St. George St., Toronto, ON M5S 1A7, Canada*
*Corresponding authors: [*]eric.zhu@utoronto.ca, [†]l.qian@utoronto.ca*

**Abstract:** A reconfigurable, multi-party quantum key distribution scheme is experimentally demonstrated by utilizing a poled fiber-based source of broadband polarization-entangled photon pairs and dense wavelength-division multiplexing (DWDM). The large bandwidth ($>$ 90 nm centered about 1555 nm) and highly spectrally-correlated nature of the entangled source is exploited to allow for the generation of more than 25 frequency-conjugate entangled pairs when aligned to the standard 200-GHz ITU grid. Such a network can serve more than 50 users simultaneously, allowing any one user on the network to establish a QKD link with any other user through wavelength-selective switching. The entangled pairs are delivered over 40 km of actual fiber (equivalent to 120 km of fiber based on channel-loss experienced), and a secure key rate of more than 20 bits/s per bi-party is observed.



**OCIS codes:** (270.5568) Quantum cryptography; (060.1810) Buffers, couplers, routers, switches, and multiplexers; (190.4370) Nonlinear optics, fibers

## References and links

1. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," Phys. Rev. Lett. **98**, 010504 (2007).
2. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek *et al.*, "Entanglement-based quantum communication over 144 km," Nature physics **3**, 481–486 (2007).
3. A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lorünser, E. Querasser, T. Matyus, H. Hübel, and A. Zeilinger, "A fully automated entanglement-based quantum cryptography system for telecom fiber networks," New Journal of Physics **11**, 045013 (2009).
4. C. H. Bennett, G. Brassard *et al.*, "Quantum cryptography: Public key distribution and coin tossing," in "Proceedings of IEEE International Conference on Computers, Systems and Signal Processing," , vol. 175 (New York, 1984), vol. 175.
5. C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," Phys. Rev. Lett. **68**, 557–559 (1992).
6. A. K. Ekert, "Quantum cryptography based on bell's theorem," Phys. Rev. Lett. **67**, 661–663 (1991).
7. C. Elliott, "Building the quantum network," New Journal of Physics **4**, 46 (2002).

8. M. Peev, C. Pacher, R. Allaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Frst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hbel, G. Humer, T. Lnger, M. Legr, R. Lieger, J. Lodewyck, T. Lornser, N. Ltkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The secoqc quantum key distribution network in vienna," New Journal of Physics **11**, 075001 (2009).
9. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the tokyo qkd network," Opt. Express **19**, 10387–10409 (2011).
10. R. J. Hughes, J. E. Nordholt, K. P. McCabe, R. T. Newell, C. G. Peterson, and R. D. Somma, "Network-centric quantum communications with application to critical infrastructure protection," arXiv preprint arXiv:1305.0305 (2013).
11. I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," New Journal of Physics **13**, 063039 (2011).
12. B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," Nature **501**, 69–72 (2013).
13. W. Chen, Z.-F. Han, T. Zhang, H. Wen, Z.-Q. Yin, F.-X. Xu, Q.-L. Wu, Y. Liu, Y. Zhang, X.-F. Mo, Y.-Z. Gui, G. Wei, and G.-C. Guo, "Field experiment on a star type metropolitan quantum key distribution network," Photonics Technology Letters, IEEE **21**, 575–577 (2009).
14. S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, L.-J. Zhang, F.-Y. Li, D. Liu, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, "Field test of wavelength-saving quantum key distribution network," Opt. Lett. **35**, 2454–2456 (2010).
15. J. Oh, C. Antonelli, and M. Brodsky, "Coincidence rates for photon pairs in wdm environment," Journal of Lightwave Technology **29**, 324–329 (2011).
16. H. C. Lim, A. Yoshizawa, H. Tsuchida, and K. Kikuchi, "Wavelength-multiplexed distribution of highly entangled photon-pairs over optical fiber," Opt. Express **16**, 22099–22104 (2008).
17. I. Herbauts, B. Blauensteiner, A. Poppe, T. Jennewein, and H. Hübel, "Demonstration of active routing of entanglement in a multi-user network," Opt. Express **21**, 29013–29024 (2013).
18. E. Y. Zhu, Z. Tang, L. Qian, L. G. Helt, M. Liscidini, J. Sipe, C. Corbari, A. Canagasabey, M. Ibsen, and P. G. Kazansky, "Direct generation of polarization-entangled photon pairs in a poled fiber," Phys. Rev. Lett. **108**, 213902 (2012).
19. M. Shtaif, C. Antonelli, and M. Brodsky, "Nonlocal compensation of polarization mode dispersion in the transmission of polarization entangled photons," Opt. Express **19**, 1728–1733 (2011).
20. H. Takesue, K. Harada, K. Tamaki, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, and S. ichi Itabashi, "Long-distance entanglement-based quantum key distribution experiment using practical detectors," Opt. Express **18**, 16777–16787 (2010).
21. S. Fasel, N. Gisin, G. Ribordy, and H. Zbinden, "Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: a comparison of two chromatic dispersion reduction methods," The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics **30**, 143–148 (2004).
22. E. Y. Zhu, Z. Tang, L. Qian, L. G. Helt, M. Liscidini, J. E. Sipe, C. Corbari, A. Canagasabey, M. Ibsen, and P. G. Kazansky, "Poled-fiber source of broadband polarization-entangled photon pairs," Opt. Lett. **38**, 4397–4400 (2013).
23. "Spectral grids for wdm applications: Dwdm frequency grid," ITU-T Recommendation G.694.1. (2012).
24. M. Avenhaus, A. Eckstein, P. J. Mosley, and C. Silberhorn, "Fiber-assisted single-photon spectrograph," Opt. Lett. **34**, 2873–2875 (2009).
25. E. Y. Zhu, C. Corbari, P. Kazansky, and L. Qian, "Self-calibrating fiber spectrometer for the measurement of broadband downconverted photon pairs," arXiv preprint arXiv:1505.01226 (2015).
26. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Information and Computation **4**, 325–360 (2004).
27. N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A **61**, 052304 (2000).
28. G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in "Advances in Cryptology EUROCRYPT 93," , vol. 765 of *Lecture Notes in Computer Science*, T. Helleseth, ed. (Springer Berlin Heidelberg, 1994), pp. 410–423.
29. L. Comandar, B. Fröhlich, J. Dynes, A. Sharpe, M. Lucamarini, Z. Yuan, R. Penty, and A. Shields, "Gigahertz-gated ingaas/inp single-photon detector with detection efficiency exceeding 55% at 1550 nm," Journal of Applied

Physics **117**, 083109 (2015).
30. A. Restelli, J. C. Bienfang, and A. L. Migdall, "Single-photon detection efficiency up to 50% at 1310 nm with an ingaas/inp avalanche diode gated at 1.25 ghz," Applied Physics Letters **102**, 141104 (2013).
31. J. Nunn, L. J. Wright, C. Söller, L. Zhang, I. A. Walmsley, and B. J. Smith, "Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion," Opt. Express **21**, 15959–15973 (2013).
32. T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits *et al.*, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," New Journal of Physics **17**, 022002 (2015).

---

Quantum key distribution (QKD) offers, in principle, an unconditionally secure method for two parties to generate a private cryptographic key. Many point-to-point (PTP) demonstrations using weak-coherent source-based [1] and entanglement-based [2, 3] quantum-cryptographic protocols such as the vaunted BB84 [4], BBM92 [5] and E91 [6] (respectively) have been demonstrated. However, PTP connections do not provide an efficient method to connect multiple users, and efforts thusfar in extending PTP links into multi-user networks have proven to be cumbersome at best.

To that end, QKD networks based upon the hub-and-spoke model, where many end-users can be connected to a trusted node [7, 8, 9, 10], are used. Should any one end-user wish to communicate with another user secretly, a random secret key is first generated at the node, then QKD is performed between the node and each user separately; finally, the key is sent to each end-user classically using the QKD key material as a one-time pad. However, the trust model for such a network topology is inherently problematic, as any security vulnerability on the node will compromise the entire network. Additionally, time-multiplexing is often required in such circumstances to service multiple users [11, 12], and only one end-user can perform QKD with the central node at a time.

Other schemes [13, 14] involving wavelength-division multiplexing (WDM) have been introduced where individual users on a PTP network can perform QKD with one another simply by addressing each other at different laser wavelengths. All users are equivalent on the network, and no central trusted node is required. However, each user must have both single photon detectors and laser sources at their disposal, and the incremental cost of adding a new user to an $N$-user network requires increasing the number of laser wavelengths available to each user to $N+1$.

In contrast, we show that a reconfigurable multi-user QKD network utilizing the distribution of polarization-entangled photon pairs from a (potentially untrustworthy) central office can be realized efficiently using a single broadband polarization-entangled source (Fig. 1). The entangled photon pairs generated from the source are highly spectrally-anticorrelated (Fig. 2), which allows for multiple ($N$) frequency-conjugate pairs to be carved out of the spectrum and distributed to $N$ ($> 25$) pairs of users simultaneously. With a $2N \times 2N$ wavelength-selective switch (WSS) to perform dynamic spectrum allocation [15], and without any additional hardware resource, any user on the network can perform QKD with any other user. Additionally, our scheme allows multiple users ($2N > 50$) to perform QKD simultaneously; when combined with time-multiplexing, such a scheme can extend the number of users well beyond what the bandwidth of the source can accommodate.

Previous works [16, 17] demonstrated the distribution of polarization-entangled photon pairs using WDM technology. However, QKD was not performed in either of those cases. Fiber spans of 10 km were used in [16], while [17] did not distribute the entangled photon pairs over any appreciable length ($> 500$ metres) of fiber. Additionally, both works employed PPLN-based correlated photon pair sources combined interferometrically (Sagnac loop in [16], and type-0 sandwich in [17]) to create entangled pairs, which are markedly more complex experimentally than the poled fiber source [18] used in this work. The usable bandwidths of both sources (10

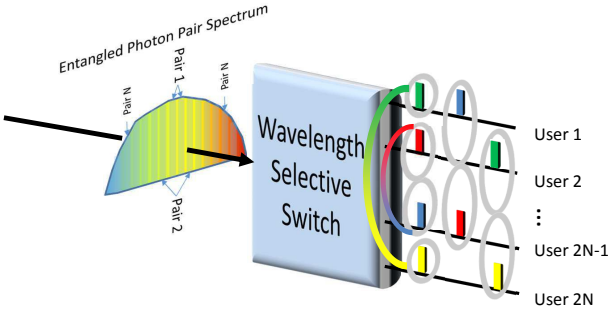


Fig. 1. The use of a broadband entangled source and a wavelength-selective switch (WSS) allows for any two parties on the network to receive frequency-conjugate polarization-entangled photon pairs. The different figure-eights denote the use of different frequency-frequency conjugate pairs to distribute entanglement to different users. The broadband nature of the source also allows for multiple simultaneous connections.

nm in [17], 55 nm in [16]) are also dwarfed by the bandwidth of the poled fiber source ($>$ 90 nm, Fig. 2). Finally, our source has a significantly higher raw entanglement fidelity ($F > 0.98$, Table 1) than either PPLN-based sources ($F < 0.94$); this means that bit-error rates due to the quality of the source are greatly reduced when poled fiber is employed for entanglement QKD.

One may argue that using polarization-entangled photon pairs to transmit a quantum key is not practical, due in part to effects such as polarization mode dispersion (PMD) causing the quality of entanglement to degrade over long fiber spans. However, we point out that nonlocal PMD cancellation is possible for polarization-entangled photons [19]. Additionally, for entanglement QKD utilizing the time-bin degree of freedom, demonstrations have either been based upon their transport in long spools of dispersion-shifted fibers [20] rather than regular single-mode fiber, such as SMF-28, or required nonlocal dispersion cancellation [21].

In this work, we employ a poled fiber-based source [18, 22] of polarization-entangled photon pairs. The source generates photon pairs in the triplet state $|\Psi^+\rangle = (|HV\rangle + |VH\rangle)/\sqrt{2}$. A Ti:Sapphire pulsed laser set to 777.45 nm is used to pump the poled fiber with a 81.6 MHz train of 400-ps-long pulses; the average power inside the poled fiber at approximately 50 mW. The broadband spectral entanglement [22] of the source is employed to distribute multiple frequency-conjugate pairs centered about 1554.9 nm (= $2 \times 777.45$ nm) to different parties. This central wavelength also happens to coincide with Channel 28 of the ITU DWDM grid [23].

Figure 2 shows the joint-spectral intensity (JSI) of the downconverted photon pairs from the poled fiber. It was measured with a fiber spectrometer [24, 25]. Due to the highly spectrally-anticorrelated nature of the downconverted photons, many frequency-conjugate pairs can be obtained simultaneously using dense wavelength division multiplexing (DWDM) technology.

The first two rows of Table 1 give the figures of merit (tangle, fidelity) of the polarization entanglement for three frequency-conjugate pairs that are spectrally separated by 3 nm, 45 nm, and 75 mm. Pair generation rates of approximately $4 \times 10^{-3}$ pairs/pulse were used to perform quantum state tomography to obtain these measurements. Each of these pairs is highlighted in Fig. 2 with a white box. While only 3 distinct conjugate pairs are used here, more than 25 bi-parties can be accomodated inside this downconversion bandwidth of the poled-fiber, assuming channel spacings of 200 GHz that are locked to the ITU grid [23]. An even greater number of biparties can be accommodated when the channel spacings are reduced to 100 GHz, or 50 GHz. We note that the ITU grid does not currently define any DWDM channels with

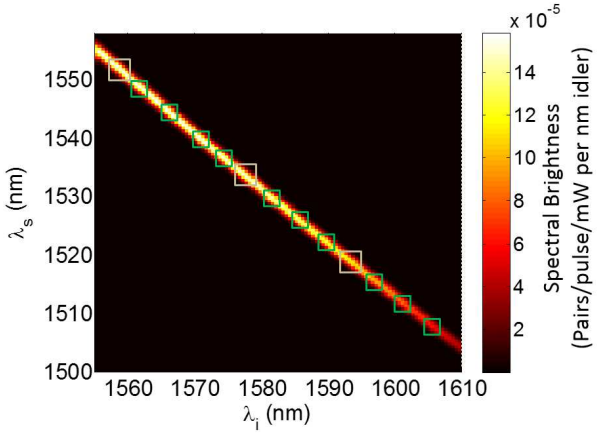


Fig. 2. (Color online.) The joint spectral intensity (JSI) of the downconverted photons is plotted as a function of the signal and idler wavelength. A total of $6.8 \times 10^{-3}$ pairs/pulse per mW of average pump power is generated over the entire spectrum. We observe that the JSI is extremely spectrally-anticorrelated. This anti-correlation allows us to separate the spectrum into many frequency-conjugate pairs (green and gray square boxes). The three pairs used in this work are highlighted by larger gray boxes. See Table 1 for the central wavelengths of each pair.

wavelengths shorter than 1520 nm. The filter centered about 1518.7 was created by cascading two coarse WDMs (CWDMs) of bandwidth 16 nm, with one centered at 1510 nm and the other centered about 1511 nm.

In our proof-of-concept demonstration of multi-user QKD, the experimental setup shown in Fig. 3a is used. A cascaded set of DWDMs is employed to spectrally-separate the signal from the idler. Each photon then traverses a 20 km spool of SMF-28 before reaching the polarization analyzers. The BBM92 [5] protocol is implemented, and experiments are run with three different frequency-conjugate signal/idler wavelength pairs (Table 1).

Each polarization analyzer consists of a 3dB (50/50) splitter that passively selects the basis in which the photon will be measured. In the top arm of the analyzer, the $H/V$ basis is measured with an unbalanced Mach-Zehnder interferometer (MZI) built from two fiber-pigtailed polarization-beam splitters (PBS); this allows for a time-multiplexed measurement scheme in which a $V$-polarized photon will arrive 2.5 ns later than an $H$-polarized photon [22]. A fiber-based polarization controller (FPC) is placed before the PBS-MZI to allow for proper polarization alignment. In the lower arm of the analyzer, a similar unbalanced MZI setup is used to measure the photon in the $D/A$ basis. The two arms are then recombined (at a loss penalty of 3 dB) so that all measurement outcomes $H/V/D/A$ can be discriminated in time and measured by a single detector (the idQuantique id220 free-running single photon detector [SPD]) for each party. This results in the mapping of the polarization degree-of-freedom onto timebins that are evenly-spaced by 2.5 ns (Fig. 3b).

There are many advantages that passive basis selection has over active basis selection. For one, there is no physical limit to the rate of switching enforced upon passive basis selection; in active switching, the use of, say, a Pockels cell will result in non-zero settling time and rise times. Secondly, the need for a random number generator to choose between bases is obviated in passive basis selection. Overall, passive basis selection reduces the complexity of the system and allows for higher speeds.

The experimental conditions are given in the third and fourth row of Table 1. These include

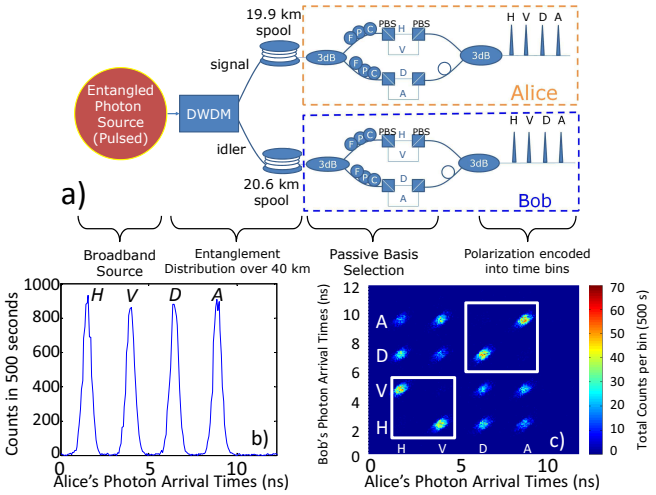


Fig. 3. (a) The full experimental setup for QKD. The signal and idler photons are separated in wavelength by a WDM before they each traverse a 20-km fiber spool and arrive at Alice and Bob's polarization analyzers. (b) During a QKD experiment, Alice tabulates the number of detector 'clicks' she receives as a function of their arrival times (with respect to the pump laser sync signal). (c) A two-dimensional histogram tabulating all the counts observed by Alice and Bob. In a real QKD implementation, only the counts for which Alice and Bob's bases coincided would be kept; these regions are highlighted by square boxes. Signal/idler WDMs centered about 1553.3/1556.65 nm are used, with a pair generation rate of $8.9 \times 10^{-3}$ pairs/pulse. The resolution of the histogram is 64 ps.

| $\lambda_s$ (nm)<br>$\lambda_i$ (nm) | 1553.3<br>1556.6 | 1533.3<br>1577.1 | 1518.7<br>1593.0 |
|---|---|---|---|
| Tangle | 0.967±0.002 | 0.964±0.004 | 0.952±0.008 |
| Fidelity to $\Psi^+$ | 0.989±0.001 | 0.989±0.001 | 0.985±0.002 |
| Pairs/pulse Generated per channel BW | $8.9 \times 10^{-3}$ | $7.6 \times 10^{-3}$ | $5.2 \times 10^{-3}$ |
| System Loss Signal+Idler: (dB) | 19.4+19.5 | 18.7+19.8 | 18.7+20.7 |
| Sifted Key Rate (bits/s) ($\pm 3\sigma$) | 32.5±0.7 | 29.4±0.7 | 16.3±0.5 |
| QBER ($\pm 3\sigma$):<br>$e_H$ (%)<br>$e_D$ (%) | <br>$2.35 \pm 0.51$<br>$2.15 \pm 0.48$ | <br>$1.68 \pm 0.45$<br>$2.23 \pm 0.51$ | <br>$4.72 \pm 1.0$<br>$7.22 \pm 1.2$ |
| Secure Key Rate (bits/s) ($\pm 3\sigma$) | $20.5 \pm 1.0$ | $19.7 \pm 1.0$ | $4.0 \pm 0.9$ |

Table 1. Entanglement QKD Results using a poled fiber as a source

the pair generation rates (which is on the order of $10^{-2}$ pairs/pulse), and system loss for signal and idler channels including detector efficiency. For each frequency-conjugate pair listed in Table 1, the acquisition time $T_{\text{acq}}$ for the QKD experiment is 500 seconds.

An electronic synchronization signal derived from the pump laser is used as a reference to

time-tag all detector events. A commercial time-to-digital converter, the PicoQuant HydraHarp 400, running in time-tagged T3 mode, is used to generate a two-dimensional histogram, which graphically tallies the arrival times of all the detector clicks (Fig. 3c) with respect to the sync signal, at a resolution of 64 ps. For each party, measurements are then binned (Fig. 3b) into 1-ns-wide time slots corresponding to the 4 measurement outcomes ($H$, $V$, $D$, and $A$). The QBER (quantum bit error rate) is then calculated from the histogrammed data. As an example, the QBER in the $H/V$ basis is calculated using the formula:

$$e_H = \frac{C_{H,H} + C_{V,V}}{C_{H,H} + C_{V,V} + C_{V,H} + C_{H,V}}, \tag{1}$$

where $C_{P_A,P_B}$ is the number of coincidence counts observed when Alice and Bob measure in the $P_A$ and $P_B$ polarizations (respectively).

The sifted key rate $R_{\text{sif}}$ is calculated using the formula:

$$R_{\text{sif}} = \frac{C_{H,V} + C_{V,H} + C_{D,D} + C_{A,A}}{T_{\text{acq}}}, \tag{2}$$

and $T_{\text{acq}}$ is the experimental acquisition time required to obtain the coincidence counts $C_{P_i,P_s}$. We note that a bit-flip must be performed for the $H/V$ coincidences to account for the anti-correlated outcomes when the state $|\Psi^+\rangle$ is used for QKD.

Finally, the secure key rate $R_{\text{sec}}$ is obtained from the formula [26]:

$$R_{\text{sec}} = R_{\text{sif}}\left(1 - \frac{1}{2}\left[h(e_H^u) + h(e_D^u)\right] - \frac{1}{2}\left[f(e_H)h(e_H) + f(e_D)h(e_D)\right]\right), \tag{3}$$

where the factor of $\frac{1}{2}$ is due to the passive basis selection being unbiased, $h(x)$ is the binary Shannon entropy ($h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$), $e_H^u$ ($e_D^u$) is the upper bound for the QBER in the $H/V$ ($D/A$) basis used to estimate the number of keys lost due to privacy amplification [27], and $f(e)$ ($\geq 1$, but taken to be 1.2 hereafter) is a measure of the efficiency of the error-correcting codes [28].

Finite key analysis is summarized in Table 1, with the QBER and $R_{\text{sec}}$ given accompanied by their uncertainties at 3 standard deviations ($\pm 3\sigma$). If we assume the fair-sampling assumption holds, a low QBER is enough to ensure the security of the key given an untrustworthy central office [26].

Excluding detection efficiencies, the channel loss (DWDMs, fiber spool attenuation, and polarization analyzers) for each photon is approximately 12 dB. This is equivalent to distributing both photons over 120 km of SMF-28 (which has a linear loss rate of 0.2 dB/km): $2\times$ 60 km = $2\times$(12 dB/[0.2 dB/km]).

We observe that secure key rates of up to 20.5 bits/s can be generated. This result is similar to rates obtained with telecom-band time-bin entangled photon pairs [20] distributed over similar lengths (50 km) of fiber (12 bits/s). However, the transport medium there was dispersion-shifted fiber, and that work only demonstrated the distribution of entangled pairs to a single pair of users.

Our key rate can also be significantly improved upon if:

- Alice and Bob each have a second detector, with one detector measuring in the $H/V$ basis and the other detector the $D/A$ basis ($\times 4$),
- splice losses due to poled-fiber and other devices were reduced ($\times 4$),
- the detector efficiencies were to increase from the current $\sim 20\%$ to 60% ($\times 9$) by utilizing practical avalanche-photodiode (APD)-based SPDs [29, 30], and

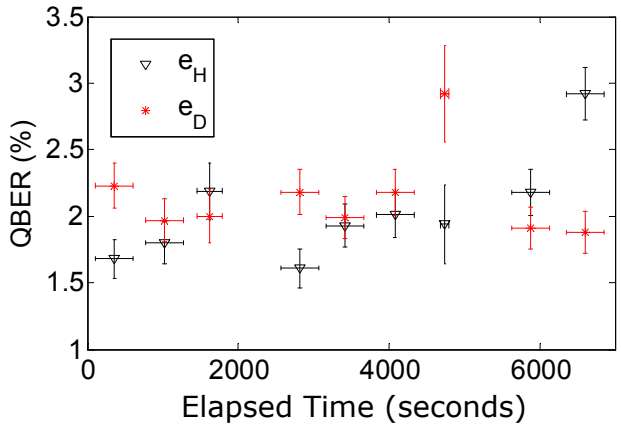


Fig. 4. Time evolution of the QBER for the 1533/1577 signal/idler set. The horizontal errorbars denote the acquisition time for each run (usually 500 seconds), while the vertical bars represent the errors (1 standard deviation) due to statistical fluctuations.

- the pump laser repetition rate were increased from 81.6 MHz to 2 GHz ($\times$25), generating photon pairs that can be detected using low-deadtime APD-based self-differencing [29] or harmonically-gated [30] SPDs.

This would result in a 3600-fold improvement in the secure-key rate to 75 kbits/s for each signal/idler channel, or an aggregate 1.5 Mbits/s when the entire spectrum of the poled fiber is utilized. In addition, the strong spectral correlations of our entangled source (Fig. 2) can be exploited for high-dimensional QKD [31], with such a scheme enabling the generation of many more than 1 secure bit per coincidence detection [32].

We also test the temporal stability of the system. For the 1533/1577 signal/idler set, the QKD system is run over a longer period of time (7000 seconds), and the QBER in each run is measured and plotted in Fig. 4. The horizontal error bars represent the integration time ($\sim$ 500 s) for each run. We observe that over this time, the QBER does not change dramatically, implying that the polarization does not drift significantly in a tabletop laboratory setting even over a 40 km spool of fiber without active polarization stabilization.

In summary, we have demonstrated the distribution of quantum keys to multiple users over standard DWDM wavelength channels by utilizing a broadband poled-fiber-based polarization-entangled source. This is the first step toward an entanglement-based, reconfigurable multi-user quantum network that is compatible (without additional resources) to current optical network infrastructures.

## 1. Acknowledgements

We acknowledge the Natural Sciences and Engineering Research Council (Canada) and the EU Project CHARMING (Contract No. FP7-288786) for funding the work presented in this paper.